

**UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF TEXAS**

DAVID SOBEL, Derivatively on Behalf of  
Nominal Defendant SOLARWINDS  
CORPORATION,

Plaintiff,

v.

KEVIN B. THOMPSON, J. BARTON  
KALSU, WILLIAM BOCK, MICHAEL  
BINGLE, SETH BORO, KENNETH Y.  
HAO, MICHAEL HOFFMAN, CATHERINE  
KINNEY, JAMES LINES, EASWARAN  
SUNDARAM, MICHAEL WIDMANN, and  
PAUL J. CORMIER,

Defendants,

and

SOLARWINDS CORPORATION,

Nominal Defendant.

Case No. 21-272

**VERIFIED STOCKHOLDER  
DERIVATIVE COMPLAINT**

Plaintiff David Sobel (“Plaintiff”), by and through his undersigned attorneys, brings this derivative complaint for the benefit of nominal defendant, SolarWinds Corporation (“SolarWinds” or the “Company”), against its Board of Directors (the “Board”) and certain of its executive officers seeking to remedy defendants’ breaches of fiduciary duties, violations of Section 14(a) of the Securities Exchange Act of 1934 (the “Exchange Act”), insider trading (*Brophy* claim), and contribution for Violations of Sections 10(b) and 21D of the Exchange Act. Plaintiff’s allegations are based upon his personal knowledge as to himself and his own acts, and upon information and belief, developed from the investigation and analysis by Plaintiff’s counsel, including a review of publicly available information, including filings by SolarWinds with the U.S. Securities and

Exchange Commission (“SEC”), press releases, news reports, analyst reports, investor conference transcripts, publicly available filings in lawsuits, and matters of public record.

## **I. NATURE AND SUMMARY OF THE ACTION**

1. SolarWinds provides software products used to monitor the health and performance of information technology networks. Its flagship product is the Orion platform, which enables oversight of network, application, and storage resources.

2. The Company’s public statements acknowledge that SolarWinds “may” be subject to cyberattacks, however failed to disclose that there were known deficiencies in its security system to protect customers’ sensitive information, and that it was not employing basic cybersecurity measures adequate to confront the risks.

3. On December 14, 2020, SolarWinds disclosed that “a vulnerability [was inserted] within its Orion monitoring products which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run.” The vulnerability was inserted in Orion products downloaded, as well as updates released, between March and June 2020. Hackers exploited the vulnerability to monitor email traffic at several U.S. government agencies and access sensitive information from over 18,000 customers.

4. On this news, the Company’s stock price fell \$3.93, or 17%, to close at \$19.62 per share on December 14, 2020, on unusually heavy trading volume.

5. On December 15, 2020, *Reuters* reported that in 2019, unknown to the public, a security researcher had alerted the Company that anyone could access SolarWinds’ update server by using the password “solarwinds123.” The article also reported that the malicious updates were still available for download even days after SolarWinds was aware their software was compromised.

6. On this news, the Company's stock price fell \$1.56, or 8%, to close at \$18.06 per share on December 15, 2020, on unusually heavy trading volume.

7. On December 17, 2020, *Bloomberg News* reported that the networks of at least three state governments had been compromised by the security breach. The networks of the U.S. Department of Energy and its National Nuclear Security Administration, which maintains the country's nuclear weapons stockpile, had also been affected by the hackers.

8. On this news, the Company's stock price fell \$3.42, or 19%, to close at \$14.18 per share on December 18, 2020.

9. On December 21, 2020, *Bloomberg News* reported that SolarWinds' executives were warned in 2017 of certain cybersecurity risks in a 23-slide presentation that cautioned that "the survival of the company depends on an internal commitment to security."

10. These revelations precipitated the filing of a securities class action in this District against SolarWinds and certain of the defendants named herein, captioned *In re SolarWinds Corporation Securities Litigation*, Case No. 21-cv-00138 (the "Securities Class Action").

11. At least half of the Company's current Board could not disinterestedly and independently respond to a litigation demand in connection with the misleading representations because, among other things, at least eight of the eleven current directors knew or recklessly ignored the deficiencies in SolarWinds' cybersecurity measures. As a result, a majority of the Board could not disinterestedly investigate whether their conduct constituted breaches of fiduciary duties under Delaware law.

## II. JURISDICTION AND VENUE

12. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1331 in that this Complaint states a federal question: violations of Section 14(a) of the Exchange Act and contribution for violations of Section 10(b) of the Exchange Act. This Court has supplemental

jurisdiction over the state law claims asserted herein pursuant to 28 U.S.C. § 1367(a). This action is not a collusive one to confer jurisdiction on a court of the United States which it would not otherwise have.

13. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391 and 1401 because a substantial portion of the transactions and wrongs complained of herein occurred in this District, and the Defendants have received substantial compensation in this district by engaging in numerous activities that had an effect in this District.

### **III. PARTIES**

#### **Plaintiff**

14. Plaintiff David Sobel purchased 4,902 shares of SolarWinds stock in January 2020 and has continuously owned his SolarWinds stock since that date.

#### **Nominal Defendant**

15. Nominal Defendant SolarWinds is a Delaware corporation with its principal executive offices located at 7171 Southwest Parkway, Building 400, Austin, Texas 78735. The Company's common stock trades on the New York Stock Exchange ("NYSE") under the symbol "SWI."

#### **Defendants**

16. Defendant Kevin B. Thompson ("Thompson") served as Chief Executive Officer ("CEO") of the Company from March 2010 to December 31, 2020 and as President of SolarWinds from January 2009 to December 31, 2020.

17. Defendant J. Barton Kalsu ("Kalsu") has served as Executive Vice President, Chief Financial Officer, and Treasurer of the Company since April 2016.

18. Defendant William Bock ("Bock") is the Chairman of the Board of Directors and has served as a director of the Company since October 2018. He is Chair of the Audit Committee.

19. Defendant Michael Bingle (“Bingle”) has served as a director of the Company since February 2016.

20. Defendant Seth Boro (“Boro”) has served as a director of the Company since February 2016.

21. Defendant Kenneth Y. Hao (“Hao”) has served as a director of the Company since February 2016.

22. Defendant Michael Hoffman (“Hoffman”) has served as a director of the Company since October 2018.

23. Defendant Catherine Kinney (“Kinney”) has served as a director of the Company since October 2018. She has served as a member of the Audit Committee.

24. Defendant James Lines (“Lines”) has served as a director of the Company since February 2016.

25. Defendant Easwaran Sundaram (“Sundaram”) has served as a director of the Company since February 2020. He has served as a member of the Audit Committee.

26. Defendant Michael Widmann (“Widmann”) has served as a director of the Company since February 2020.

27. Defendant Paul J. Cormier (“Cormier”) served as a director of the Company from October 2018 to September 2020.

28. Defendants Thompson, Kalsu, Bock, Bingle, Boro, Hao, Hoffman, Kinney, Lines, Sundaram, Widmann, and Cormier are sometimes referred to hereinafter as the “Individual Defendants.”

### **Relevant Non-Party**

29. Sudhakar Ramakrishna (“Ramakrishna”) has served as CEO and as a director of the Company since January 2021.

30. Dennis Howard (“Howard”) has served as a director of the Company since September 2020. He is a member of the Audit Committee.

### **IV. DUTIES OF THE INDIVIDUAL DEFENDANTS**

31. By reason of their positions as officers, directors, and/or fiduciaries of SolarWinds and because of their ability to control the business and corporate affairs of SolarWinds, at all relevant times, the Individual Defendants owed SolarWinds and its shareholders fiduciary obligations of good faith, loyalty, and candor, and were required to use their utmost ability to control and manage SolarWinds in a fair, just, honest, and equitable manner. The Individual Defendants were required to act in furtherance of the best interests of SolarWinds and its shareholders so as to benefit all shareholders equally and not in furtherance of their personal interest or benefit. Each director and officer of the Company owes to SolarWinds and its shareholders a fiduciary duty to exercise good faith and diligence in the administration of the affairs of the Company and in the use and preservation of its property and assets, and the highest obligations of fair dealing.

32. The Individual Defendants, because of their positions of control and authority as directors and/or officers of SolarWinds, were able to and did, directly and/or indirectly, exercise control over the wrongful acts complained of herein. Because of their advisory, executive, managerial, and directorial positions with SolarWinds, each of the Individual Defendants had knowledge of material non-public information regarding the Company.

33. To discharge their duties, the officers and directors of SolarWinds were required to exercise reasonable and prudent supervision over the management, policies, practices and controls

of the Company. By virtue of such duties, the officers and directors of SolarWinds were required to, among other things:

- (a) Exercise good faith to ensure that the affairs of the Company were conducted in an efficient, business-like manner so as to make it possible to provide the highest quality performance of their business;
- (b) Exercise good faith to ensure that the Company was operated in a diligent, honest, and prudent manner and complied with all applicable federal and state laws, rules, regulations and requirements, and all contractual obligations, including acting only within the scope of its legal authority;
- (c) Exercise good faith to ensure that the Company's communications with the public and with shareholders are made with due candor in a timely and complete fashion; and
- (d) When put on notice of problems with the Company's business practices and operations, exercise good faith in taking appropriate action to correct the misconduct and prevent its recurrence.

## **V. SUBSTANTIVE ALLEGATIONS**

### **A. Background**

34. SolarWinds provides software products used to monitor the health and performance of information technology networks and serves over 300,000 customers.

35. The Company's flagship product is its Orion platform, which enables oversight of network, application, and storage resources. Orion is widely used by U.S. government agencies and Fortune 500 companies. The platform accounts for nearly half of the Company's annual revenue. Orion requires unrestricted access to customers' networks, including sensitive administrative credentials.

### **B. The Individual Defendants Cause the Company to Issue Materially Misleading Statements**

36. On September 21, 2018, defendants Thompson, Kalsu, Boro, Lines, Hao, Bingle, and non-party director Jason White signed and caused SolarWinds to file a registration statement for its initial public offering ("IPO").

37. On October 18, 2018, the Registration Statement, following certain amendments, was declared effective by the SEC. On or about October 19, 2018, the Company completed its IPO pursuant to the registration statement, selling 28,750,000 million shares for \$15 per share. On October 22, 2018, the Individual Defendants caused SolarWinds to file its prospectus for the IPO on Form 424B4, which incorporated and formed part of the IPO registration statement (collectively, the “IPO Offering Materials”). Regarding the Company’s cybersecurity measures, the IPO Offering Materials stated, in relevant part:<sup>1</sup>

*Because the techniques used to obtain unauthorized access or to sabotage systems change frequently and generally are not identified until they are launched against a target, we may be unable to anticipate these techniques or to implement adequate preventative measures. We may also experience security breaches that may remain undetected for an extended period and, therefore, have a greater impact on the products we offer, the proprietary data contained therein, and ultimately on our business.*

*The foregoing security problems could result in, among other consequences, damage to our own systems or our customers’ IT infrastructure or the loss or theft of our customers’ proprietary or other sensitive information.* The costs to us to eliminate or address the foregoing security problems and security vulnerabilities before or after a cyber incident could be significant. Our remediation efforts may not be successful and could result in interruptions, delays or cessation of service and loss of existing or potential customers that may impede sales of our products or other critical functions. We could lose existing or potential customers in connection with any actual or perceived security vulnerabilities in our websites or our products.

During the purchasing process and in connection with evaluations of our software, either we or third-party providers collect and use customer information, including personally identifiable information, such as credit card numbers, email addresses, phone numbers and IP addresses. We have legal and contractual obligations to protect the confidentiality and appropriate use of customer data. *Despite our security measures, unauthorized access to, or security breaches of, our software or systems could result in the loss, compromise or corruption of data, loss of business, severe reputational damage adversely affecting customer or investor confidence, regulatory investigations and orders, litigation, indemnity obligations, damages for contract breach, penalties for violation of applicable laws or regulations, significant costs for remediation and other liabilities.* We

---

<sup>1</sup> Unless otherwise stated, all emphasis in bold and italics hereinafter is added.



have incurred and expect to incur significant expenses to prevent security breaches, including deploying additional personnel and protection technologies, training employees, and engaging third-party experts and consultants. Our errors and omissions insurance coverage covering certain security and privacy damages and claim expenses may not be sufficient to compensate for all liabilities we incur.

38. On November 27, 2018, defendants Thompson, Kalsu, Bock, Bingle, Boro, Cormier, Hao, Hoffman, Kinney, and Lines caused SolarWinds to file its quarterly report on Form 10-Q for the period ended September 30, 2018 with the SEC. It incorporated by reference the representations regarding the Company's cybersecurity risks, as set forth in ¶ 37.

39. On February 25, 2019, defendants Thompson, Kalsu, Bock, Bingle, Boro, Cormier, Hao, Hoffman, Kinney, and Lines signed and caused SolarWinds to file its annual report on Form 10-K with the SEC for the period ended December 31, 2018 (the "2018 10-K"). Regarding the Company's cybersecurity risks, the report stated, in relevant part:

***Because the techniques used to obtain unauthorized access or to sabotage systems change frequently and generally are not identified until they are launched against a target, we may be unable to anticipate these techniques or to implement adequate preventative measures. We may also experience security breaches that may remain undetected for an extended period and, therefore, have a greater impact on the products we offer, the proprietary data contained therein, and ultimately on our business.***

***The foregoing security problems could result in, among other consequences, damage to our own systems or our customers' IT infrastructure or the loss or theft of our customers' proprietary or other sensitive information.*** The costs to us to eliminate or address the foregoing security problems and security vulnerabilities before or after a cyber incident could be significant. Our remediation efforts may not be successful and could result in interruptions, delays or cessation of service and loss of existing or potential customers that may impede sales of our products or other critical functions. We could lose existing or potential customers in connection with any actual or perceived security vulnerabilities in our websites or our products.

During the purchasing process and in connection with evaluations of our software, either we or third-party providers collect and use customer information, including personally identifiable information, such as credit card numbers, email addresses, phone numbers and IP addresses. We have legal and contractual obligations to protect the confidentiality and appropriate use of customer data. ***Despite our security measures, unauthorized access to, or security breaches of, our software***

*or systems could result in the loss, compromise or corruption of data, loss of business, severe reputational damage adversely affecting customer or investor confidence, regulatory investigations and orders, litigation, indemnity obligations, damages for contract breach, penalties for violation of applicable laws or regulations, significant costs for remediation and other liabilities.* We have incurred and expect to incur significant expenses to prevent security breaches, including deploying additional personnel and protection technologies, training employees, and engaging third-party experts and consultants. Our errors and omissions insurance coverage covering certain security and privacy damages and claim expenses may not be sufficient to compensate for all liabilities we incur.

40. On April 5, 2019, the Individual Defendants caused the Company to file its proxy statement soliciting votes for several management proposals at the Company's annual stockholder meeting set for May 16, 2019. Although SolarWinds is a controlled company,<sup>2</sup> the proxy statement assured shareholders that "[y]our vote is important." By its terms, the proxy statement, which was signed by defendant Thompson, was issued "by order of the Board of Directors." Among other things, the proxy statement disclosed:

#### **Risk Oversight**

Our Board is responsible for overseeing our risk management process. The Board does not have a standing risk management committee, but rather administers this oversight function primarily through our nominating and corporate governance committee. The Board is also apprised of particular risk management matters in connection with its general oversight and approval of corporate matters and significant transactions.

Our nominating and corporate governance committee is responsible for our general risk management strategy, monitoring and assessing the most significant risks facing us and overseeing the implementation of risk mitigation strategies by management. Our nominating and corporate governance committee also monitors and assesses the effectiveness of our corporate governance guidelines and our

---

<sup>2</sup> SolarWinds is controlled by the Silver Lake Funds and the Thoma Bravo Funds (together, the "Sponsors"), which owned 44.4% and 36.2%, respectively, of the Company's outstanding stock as of March 22, 2019. "Silver Lake Funds" refers to Silver Lake Parnets IV, L.P., Silver Lake Technology Investors IV, L.P., and SLP Aurora Co-Invest, L.P. "Thoma Bravo Funds" refers to Thoma Bravo Fund XI, L.P., Thoma Bravo Fund XI-A, L.P., Thoma Bravo Fund XII, L.P., Thoma Bravo Fund XII-A, L.P., Thoma Bravo Executive Fund XI, L.P., Thoma Bravo Executive Fund XII, L.P., Thoma Bravo Executive Fund XII-a, L.P., Thoma Bravo Special Opportunities Fund II, L.P. and Thoma Bravo Special Opportunities Fund II-A, L.P.

policies, plans and programs relating to cyber and data security and legal and regulatory risks associated with our products and business operations.

41. According to the proxy statement, at the time of filing the Nominating and Corporate Governance Committee was comprised of defendants Bingle, Cormier, and Kinney and during 2018, “our nominating and corporate governance committee held one meeting.”

42. The proxy statement was materially misleading as to the Board’s oversight of risk because the nominating and corporate governance committee was only empowered to act as to nominating functions and eleven “corporate governance functions,” none of which included the oversight of any enterprise risks. Specifically, the nominating and governance committee charter provides that:

The primary responsibilities of the Committee are to (i) identify individuals qualified to become Board members; (ii) select, or recommend to the Board, director nominees for each election of directors; (iii) develop and recommend to the Board criteria for selecting qualified director candidates; (iv) consider committee member qualifications, appointment and removal; (v) recommend corporate governance principles and a code of conduct applicable to the Company; and (vi) provide oversight in the evaluation of the Board and each committee.

43. As a result of the material misstatements and omissions contained in the proxy statement, Company shareholders re-elected defendants Thompson, Bock, Boro, and Hao as directors. The misleading statements in the proxy statement were a fundamental link in the Individual Defendants’ continued breaches of fiduciary duties, and caused SolarWinds’ shareholders to forego remedies available to them under Delaware law, such as suing to halt the vote, that they would have pursued had the truth been disclosed.

44. On May 10, 2019, defendants Thompson, Kalsu, Bock, Bingle, Boro, Cormier, Hao, Hoffman, Kinney, and Lines caused SolarWinds to file its quarterly report on Form 10-Q for the period ended March 31, 2019. It was signed by defendants Thompson and Kalsu attesting to the accuracy and completeness of the report. The report also incorporated by reference the

representations regarding the Company's cybersecurity risks from the 2018 10-K, as set forth in 39.

45. On or about May 22, 2019, SolarWinds conducted a secondary public offering ("SPO") pursuant to a registration statement filed on May 20, 2019 and signed by defendants Thompson, Kalsu, Bock, Bingle, Boro, Cormier, Hao, Hoffman, Kinney, and Lines. On May 23, 2019, SolarWinds filed a prospectus for the SPO on Form 424B4 with the SEC (with the SPO registration statement, the "SPO Offering Materials"). Regarding the Company's cybersecurity risks, the SPO Materials stated, in relevant part:

*Because the techniques used to obtain unauthorized access or to sabotage systems change frequently and generally are not identified until they are launched against a target, we may be unable to anticipate these techniques or to implement adequate preventative measures. We may also experience security breaches that may remain undetected for an extended period and, therefore, have a greater impact on the products we offer, the proprietary data contained therein, and ultimately on our business.*

*The foregoing security problems could result in, among other consequences, damage to our own systems or our customers' IT infrastructure or the loss or theft of our customers' proprietary or other sensitive information.* The costs to us to eliminate or address the foregoing security problems and security vulnerabilities before or after a cyber incident could be significant. Our remediation efforts may not be successful and could result in interruptions, delays or cessation of service and loss of existing or potential customers that may impede sales of our products or other critical functions. We could lose existing or potential customers in connection with any actual or perceived security vulnerabilities in our websites or our products.

During the purchasing process and in connection with evaluations of our software, either we or third-party providers collect and use customer information, including personally identifiable information, such as credit card numbers, email addresses, phone numbers and IP addresses. We have legal and contractual obligations to protect the confidentiality and appropriate use of customer data. *Despite our security measures, unauthorized access to, or security breaches of, our software or systems could result in the loss, compromise or corruption of data, loss of business, severe reputational damage adversely affecting customer or investor confidence, regulatory investigations and orders, litigation, indemnity obligations, damages for contract breach, penalties for violation of applicable laws or regulations, significant costs for remediation and other liabilities.* We have incurred and expect to incur significant expenses to prevent security breaches,

including deploying additional personnel and protection technologies, training employees, and engaging third-party experts and consultants. Our errors and omissions insurance coverage covering certain security and privacy damages and claim expenses may not be sufficient to compensate for all liabilities we incur.

46. On August 12, 2019, defendants Thompson, Kalsu, Bock, Bingle, Boro, Cormier, Hao, Hoffman, Kinney, and Lines caused SolarWinds to file its quarterly report on Form 10-Q for the period ended June 30, 2019. It was signed by defendants Thompson and Kalsu attesting to the accuracy and completeness of the report. The report also incorporated by reference the representations regarding the Company's cybersecurity risks from the 2018 10-K, as set forth in ¶ 39.

47. On November 7, 2019, defendants Thompson, Kalsu, Bock, Bingle, Boro, Cormier, Hao, Hoffman, Kinney, and Lines caused SolarWinds to file its quarterly report on Form 10-Q for the period ended September 30, 2019. It was signed by defendants Thompson and Kalsu attesting to the accuracy and completeness of the report. The report also incorporated by reference the representations regarding the Company's cybersecurity risks from the 2018 10-K, as set forth in ¶ 39.

48. On February 24, 2020, defendants Thompson, Kalsu, Bock, Bingle, Boro, Cormier, Hao, Hoffman, Kinney, and Lines signed and caused SolarWinds to file its annual report on Form 10-K with the SEC for the period ended December 31, 2019 (the "2019 10-K"). Regarding the Company's cybersecurity risks, the report stated, in relevant part:

We are heavily dependent on our technology infrastructure to sell our products and operate our business, and our customers rely on our technology to help manage their own IT infrastructure. Our systems and those of our third-party service providers are vulnerable to damage or interruption from natural disasters, fire, power loss, telecommunication failures, traditional computer "hackers," malicious code (such as viruses and worms), employee or contractor theft or misuse, and denial-of-service attacks, as well as sophisticated nation-state and nation-state-supported actors (including advanced persistent threat intrusions). The risk of a security breach or disruption, particularly through cyberattacks or cyber intrusion, including by computer hacks, foreign governments, and cyber terrorists, has

generally increased the number, intensity and sophistication of attempted attacks, and intrusions from around the world have increased. In addition, sophisticated hardware and operating system software and applications that we procure from third parties may contain defects in design or manufacture, including “bugs” and other problems that could unexpectedly interfere with the operation of our systems

***Because the techniques used to obtain unauthorized access or to sabotage systems change frequently and generally are not identified until they are launched against a target, we may be unable to anticipate these techniques or to implement adequate preventative measures. We may also experience security breaches that may remain undetected for an extended period and, therefore, have a greater impact on the products we offer, the proprietary data contained therein, and ultimately on our business.***

***The foregoing security problems could result in, among other consequences, damage to our own systems or our customers’ IT infrastructure or the loss or theft of our customers’ proprietary or other sensitive information.*** The costs to us to eliminate or address the foregoing security problems and security vulnerabilities before or after a cyber incident could be significant. Our remediation efforts may not be successful and could result in interruptions, delays or cessation of service and loss of existing or potential customers that may impede sales of our products or other critical functions. We could lose existing or potential customers in connection with any actual or perceived security vulnerabilities in our websites or our products.

During the purchasing process and in connection with evaluations of our software, either we or third-party providers collect and use customer information, including personally identifiable information, such as credit card numbers, email addresses, phone numbers and IP addresses. We have legal and contractual obligations to protect the confidentiality and appropriate use of customer data. ***Despite our security measures, unauthorized access to, or security breaches of, our software or systems could result in the loss, compromise or corruption of data, loss of business, severe reputational damage adversely affecting customer or investor confidence, regulatory investigations and orders, litigation, indemnity obligations, damages for contract breach, penalties for violation of applicable laws or regulations, significant costs for remediation and other liabilities.*** We have incurred and expect to incur significant expenses to prevent security breaches, including deploying additional personnel and protection technologies, training employees, and engaging third-party experts and consultants. Our errors and omissions insurance coverage covering certain security and privacy damages and claim expenses may not be sufficient to compensate for all liabilities we incur.

49. On April 9, 2020, the Individual Defendants caused the Company to file its proxy statement soliciting votes for several management proposals at the Company’s annual stockholder

meeting set for May 21, 2020. Although SolarWinds is a controlled company,<sup>3</sup> the proxy statement assured shareholders that “[y]our vote is important.” By its terms, the proxy statement, which was signed by defendant Thompson, was issued “by order of the Board of Directors.” Among other things, the proxy statement disclosed:

### **Risk Oversight**

Our Board is responsible for overseeing our risk management process. The Board does not have a standing risk management committee, but rather administers this oversight function primarily through our nominating and corporate governance committee. The Board is also apprised of particular risk management matters in connection with its general oversight and approval of corporate matters and significant transactions.

Our nominating and corporate governance committee is responsible for our general risk management strategy, monitoring and assessing the most significant risks facing us and overseeing the implementation of risk mitigation strategies by management. Our nominating and corporate governance committee also monitors and assesses the effectiveness of our corporate governance guidelines and our policies, plans and programs relating to cyber and data security and legal and regulatory risks associated with our products and business operations.

50. According to the proxy statement, at the time of filing the Nominating and Corporate Governance Committee was comprised of defendants Bingle, Cormier, and Kinney and during 2019, “our nominating and corporate governance committee held three meetings.”

51. The proxy statement was materially misleading as to the Board’s oversight of risk because the nominating and corporate governance committee was only empowered to act as to nominating functions and eleven “corporate governance functions,” none of which included the oversight of any enterprise risks. Specifically, the nominating and governance committee charter provides that:

---

<sup>3</sup> SolarWinds is controlled by the Silver Lake Funds, the Thoma Bravo Funds, and the Thoma Bravo Co-Investors, which owned 41.7%, 34.0%, and 7.7%, respectively, of the Company’s outstanding stock as of March 31, 2020.



The primary responsibilities of the Committee are to (i) identify individuals qualified to become Board members; (ii) select, or recommend to the Board, director nominees for each election of directors; (iii) develop and recommend to the Board criteria for selecting qualified director candidates; (iv) consider committee member qualifications, appointment and removal; (v) recommend corporate governance principles and a code of conduct applicable to the Company; and (vi) provide oversight in the evaluation of the Board and each committee.

52. As a result of the material misstatements and omissions contained in the proxy statement, Company shareholders re-elected defendants Kinney, Lines, Sundaram, and Widmann as directors. The misleading statements in the proxy statement were a fundamental link in the Individual Defendants' continued breaches of fiduciary duties, and caused SolarWinds' shareholders to forego remedies available to them under Delaware law, such as suing to halt the vote, that they would have pursued had the truth been disclosed.

53. On May 8, 2020, the Individual Defendants caused SolarWinds to file its quarterly report on Form 10-Q for the period ended March 31, 2020. It was signed by defendants Thompson and Kalsu attesting to the accuracy and completeness of the report. The report also incorporated by reference the representations regarding the Company's cybersecurity risks from the 2019 10-K, as set forth in ¶ 48.

54. On August 10, 2020, the Individual Defendants caused SolarWinds to file its quarterly report on Form 10-Q for the period ended June 30, 2020. It was signed by defendants Thompson and Kalsu attesting to the accuracy and completeness of the report. The report also incorporated by reference the representations regarding the Company's cybersecurity risks from the 2019 10-K, as set forth in ¶ 48.

55. On November 5, 2020, defendants Thompson, Kalsu, Bock, Bingle, Boro, Cormier, Hao, Hoffman, Kinney, Lines, Sundaram, and Widmann caused SolarWinds to file its quarterly report on Form 10-Q for the period ended September 30, 2020. It was signed by defendants Thompson and Kalsu attesting to the accuracy and completeness of the report. The report also



incorporated by reference the representations regarding the Company's cybersecurity risks from the 2019 10-K, as set forth in ¶ 48.

56. The above statements in ¶¶ 36-39, 44-48, 53-55 were materially misleading because they failed to disclose that: (1) SolarWinds failed to maintain adequate security measures and effective monitoring systems to sufficiently protect against security threats; (2) that, among other things, the Company's update server used an easily accessible password 'solarwinds123'; (3) that, as a result, a significant portion of the Company's customers were vulnerable to cyberattacks, resulting in reputational harm to SolarWinds.

### **C. The Truth Emerges**

57. On December 13, 2020, *Reuters* reported hackers have been monitoring email traffic at the U.S. Treasury and Commerce departments. The hackers are believed to have breached the emails by deceptively interfering with updates released by SolarWinds, which services various government vendors in the executive branch, the military, and the intelligence services. The hackers inserted malicious code into Orion software updates affecting nearly 18,000 customers.

58. On December 14, 2020, the Company disclosed that "a vulnerability [was inserted] within its Orion monitoring products which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run." The vulnerability was inserted in Orion products downloaded, as well as updates released, between March and June 2020. Specifically, SolarWinds filed a Form 8-K with the SEC, stating in relevant part:

***SolarWinds Corporation ("SolarWinds" or the "Company") has been made aware of a cyberattack that inserted a vulnerability within its Orion monitoring products which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run.*** SolarWinds has been advised that this incident was likely the result of a highly sophisticated, targeted and manual supply chain attack by an outside nation state, but SolarWinds has not independently verified the identity of the attacker. SolarWinds has retained third-party cybersecurity experts to assist in an investigation of these matters, including whether a vulnerability in the Orion monitoring products was exploited as a point

of any infiltration of any customer systems, and in the development of appropriate mitigation and remediation plans. SolarWinds is cooperating with the Federal Bureau of Investigation, the U.S. intelligence community, and other government agencies in investigations related to this incident.

***Based on its investigation to date, SolarWinds has evidence that the vulnerability was inserted within the Orion products and existed in updates released between March and June 2020 (the “Relevant Period”), was introduced as a result of a compromise of the Orion software build system and was not present in the source code repository of the Orion products.*** SolarWinds has taken steps to remediate the compromise of the Orion software build system and is investigating what additional steps, if any, should be taken. SolarWinds is not currently aware that this vulnerability exists in any of its other products.

SolarWinds currently believes that:

- Orion products downloaded, implemented or updated during the Relevant Period contained the vulnerability;
- Orion products downloaded and implemented before the Relevant Period and not updated during the Relevant Period did not contain the vulnerability;
- Orion products downloaded and implemented after the Relevant Period did not contain the vulnerability; and
- Previously affected versions of the Orion products that were updated with a build released after the Relevant Period no longer contained the vulnerability; however, the server on which the affected Orion products ran may have been compromised during the period in which the vulnerability existed.

SolarWinds values the privacy and security of its over 300,000 customers and is working closely with customers of its Orion products to address this incident. On December 13, 2020, ***SolarWinds delivered a communication to approximately 33,000 Orion product customers that were active maintenance customers during and after the Relevant Period. SolarWinds currently believes the actual number of customers that may have had an installation of the Orion products that contained this vulnerability to be fewer than 18,000.*** The communication to these customers contained mitigation steps, including making available a hotfix update to address this vulnerability in part and additional measures that customers could take to help secure their environments. SolarWinds is also preparing a second hotfix update to further address the vulnerability, which SolarWinds currently expects to release on or prior to December 15, 2020. For the nine months ended September 30, 2020, total revenue from the Orion products across all customers, including those who may have had an installation of the Orion products that contained this

vulnerability, was approximately \$343 million, or approximately 45% of total revenue.

There has been significant media coverage of attacks on U.S. governmental agencies and other companies, with many of those reports attributing those attacks to a vulnerability in the Orion products. SolarWinds is still investigating whether, and to what extent, a vulnerability in the Orion products was successfully exploited in any of the reported attacks.

59. On this news, the Company's stock price fell \$3.93, or 17%, to close at \$19.62 per share on December 14, 2020, on unusually heavy trading volume.

60. On December 15, 2020, *Reuters* reported that Vinoth Kumar, a security researcher, alerted the Company last year that anyone could access SolarWinds' update server by using the password "solarwinds123." The article also reported that co-founder of cybersecurity company Huntress, Kyle Hanslovan, noticed the malicious updates were still available for download even days after SolarWinds was aware their software was compromised.

61. On this news, the Company's stock price fell \$1.56, or 8%, to close at \$18.06 per share on December 15, 2020, on unusually heavy trading volume.

62. On December 17, 2020, *Bloomberg News* reported that the networks of at least three state governments had been compromised by the security breach. The networks of the U.S. Department of Energy and its National Nuclear Security Administration, which maintains the country's nuclear weapons stockpile, had also been affected by the hackers.

63. On this news, the Company's stock price fell \$3.42, or 19%, to close at \$14.18 per share on December 18, 2020.

64. On December 21, 2020, *Bloomberg News* reported that SolarWinds' executives were warned in 2017 of certain cybersecurity risks. According to the article, a former SolarWinds cybersecurity advisor, Ian Thornton-Trump, delivered a 23-slide presentation to at least three of the company's advisors warning them that "the survival of the company depends on an internal

commitment to security.” According to Thornton-Trump, “SolarWinds was an incredibly easy target to hack,” but management was “unwilling to make the corrections” necessary to improve the deficient security measures. Despite knowing the increasing prevalence of hackers since at least 2015, “SolarWinds did not adapt” and “wasn’t paying attention to what was going on.” According to a former SolarWinds software engineer, the Company prioritized new products over its internal cybersecurity protections and the internal systems ran out-of-date web browsers and operating systems. As a result, Thornton-Trump and the software engineer “viewed a major breach [of SolarWinds] as inevitable.”

65. On March 1, 2021, the Company filed its Form 10-K for the 2020 and disclosed in part the following:

On December 14, 2020, we announced that we had been the victim of a cyberattack on our Orion Software Platform and internal systems, or the “Cyber Incident.” Together with outside security professionals and other third parties, we are conducting investigations into the Cyber Incident which are on-going.

Our investigations to date revealed that as part of this attack, malicious code, or Sunburst, was injected into builds of our Orion Software Platform that we released between March 2020 and June 2020. If present and activated in a customer’s IT environment, Sunburst could potentially allow an attacker to compromise the server on which the Orion Software Platform was installed. We have not located Sunburst in any of our more than seventy non-Orion products and tools.

We released remediations for the versions of our Orion Software Platform known to be affected by Sunburst and have taken and continue to take extensive efforts to support and protect our customers. In addition, we shared our proprietary code with industry researchers to enable them to validate a “kill-switch” that is believed to have rendered Sunburst inert.

The Orion Software Platform is installed “on-premises” within customers’ IT environments, so we are unable to determine with specificity the number of customers that installed an affected version or that were compromised as a result of Sunburst. We believe the actual number of customers that could have installed an affected version of the Orion Software Platform to be fewer than 18,000. Based on our discussions with customers and our investigations into the nature and function of Sunburst and the tradecraft of the threat actor, we believe the number of organizations which were exploited by the threat actors through Sunburst to be

substantially fewer than the number of customers that may have installed an affected version of the Orion Platform.

It has been widely reported that, due to its nature, sophistication and operational security, this “supply-chain” cyberattack was part of a broader nation-state level cyber operation designed to target public and private sector organizations. As of the date hereof, we have not independently attributed the Cyber Incident to any specific threat actor.

Through our investigations into the Cyber Incident, we hope to understand it better, apply our findings to further adapt and enhance our security measures across our systems and our software development and build environments and share our findings and adaptations with our customers, government officials and the technology industry more broadly to help them better understand and protect against these types of attacks in the future. We refer to these adaptations and enhancements as “Secure by Design.

**D. Thompson, Bingle, Kalsu, and Lines Sold More than \$300 Million in SolarWinds Stock While in Possession of Material Non-Public Information**

Thompson

66. Defendant Thompson was the Company’s CEO with a highly sophisticated understanding of the Company’s cybersecurity risks.

67. As set forth herein, as early as 2017, defendant Thompson possessed material negative information which he knew was being concealed from investors. Defendant Thompson consciously acted to exploit his knowledge by selling nearly \$11 million of SolarWinds stock to his substantial benefit, as follows:

Date	Shares	Price	Proceeds
8/11/2020	58,634	\$19.48	\$1,142,483
8/11/2020	300,000	\$19.52	\$5,856,000
11/18/2020	175,000	\$21.60	\$3,780,000
	<b>533,624</b>		<b>\$10,778,483</b>

68. Defendant Thompson thus used his fiduciary position to enrich himself and failed to discharge his duties by causing the Company to candidly reveal the truth of its business condition.

Bingle

69. Defendant Bingle is a director of the Company with a highly sophisticated understanding of the Company's cybersecurity risks.

70. As set forth herein, as early as 2017, defendant Bingle possessed material negative information which he knew was being concealed from investors. Defendant Bingle consciously acted to exploit his knowledge by selling over \$288 million of SolarWinds stock to his substantial benefit, as follows:

<b>Date</b>	<b>Shares</b>	<b>Price</b>	<b>Proceeds</b>
5/28/2019	7,500,000	\$17.42	\$130,612,500
12/7/2020	7,168,866	\$21.97	\$157,499,986
	<b>14,668,866</b>		<b>\$288,112,486</b>

71. Defendant Bingle thus used his fiduciary position to enrich himself and failed to discharge his duties by causing the Company to candidly reveal the truth of its business condition.

Kalsu

72. Defendant Kalsu is CFO of the Company with a highly sophisticated understanding of the Company's cybersecurity risks

73. As set forth herein, as early as 2017, defendant Kalsu possessed material negative information which he knew was being concealed from investors. Defendant Kalsu consciously acted to exploit his knowledge by selling over \$1.6 million worth of SolarWinds stock to his substantial benefit: on May 21, 2020, he sold 95,432 shares for \$17.69 per share and received proceeds of \$1,688,192.

74. Defendant Kalsu thus used his fiduciary position to enrich himself and failed to discharge his duties by causing the Company to candidly reveal the truth of its business condition.

Lines

75. Defendant Lines is a director of the Company with a highly sophisticated understanding of the Company's cybersecurity risks

76. As set forth herein, as early as 2017, defendant Lines possessed material negative information which he knew was being concealed from investors. Defendant Lines consciously acted to exploit his knowledge by selling over \$380,000 worth of SolarWinds stock to his substantial benefit: on August 31, 2020, he sold 18,333 shares for \$21.12 per share and received proceeds of \$387,193.

77. Defendant Lines thus used his fiduciary position to enrich himself and failed to discharge his duties by causing the Company to candidly reveal the truth of its business condition.

**VI. DAMAGES TO THE COMPANY**

78. As a direct and proximate result of the Individual Defendants' conduct, SolarWinds has been seriously harmed and will continue to be. Such harm includes, but is not limited to:

- a) Liability to the Company from the numerous lawsuits filed as a result of the massive hack of SolarWinds products;
- b) Ill-gotten gains from their insider selling; and
- c) Costs incurred from compensation and benefits paid to the defendants who have breached their duties to SolarWinds.

79. In addition, SolarWinds's business, goodwill, and reputation with its business partners, regulators, and shareholders have been gravely impaired. The Company still has not fully admitted the nature of its false statements and the true condition of its business. The credibility and motives of management are now in serious doubt.

80. The actions complained of herein have irreparably damaged SolarWinds's corporate image and goodwill. For at least the foreseeable future, SolarWinds will suffer from

what is known as the “liar’s discount,” a term applied to the stocks of companies who have been implicated in illegal behavior and have misled the investing public, such that SolarWinds’s ability to raise equity capital or debt on favorable terms in the future is now impaired.

## **VII. DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS**

81. Plaintiff brings this action derivatively in the right and for the benefit of SolarWinds to redress injuries suffered, and to be suffered, by SolarWinds as a direct result of breaches of fiduciary duty by the Individual Defendants, violations of Section 14(a) of the Exchange Act, insider trading, and contribution for violations of Section 10(b) of the Exchange Act. SolarWinds is named as a nominal defendant solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have.

82. Plaintiff will adequately and fairly represent the interests of SolarWinds in enforcing and prosecuting its rights.

83. Plaintiff has continuously been a shareholder of SolarWinds at times relevant to the wrongdoing complained of and is a current SolarWinds shareholder.

84. When this action was filed, SolarWinds’s Board of Directors consisted of defendants Bock, Bingle, Boro, Hao, Hoffman, Kinney, Lines, Sundaram, and Widmann, and non-party directors Ramakrishna and Howard. Plaintiff did not make any demand on the Board to institute this action because such a demand would be a futile, wasteful, and useless act, as set forth below.

### **A. The Board Failed to Oversee Cyber and Data Security Risks**

85. Bock, Bingle, Boro, Hao, Hoffman, Kinney, Lines, Sundaram, and Widmann failed to ensure that the Board exercised adequate oversight of cyber and data security risks associated with SolarWinds’ products and business. According to SolarWinds’ proxy statements, the Nominating and Corporate Governance Committee was responsible for “[SolarWinds’] risk



management strategy, monitoring and assessing the most significant risks facing us and overseeing the implementation of risk mitigation strategies.” The Nominating and Corporate Governance Committee, according to the proxy statements, “monitors and assesses the effectiveness of our corporate governance guidelines and our policies, plans and programs relating to cyber and data security and legal and regulatory risks associated with our products and business operations.” Due to the nature of the Company’s business, the Company’s policies, plans and programs relating to cyber and data security associated with SolarWinds’ products and business operations SolarWinds’ most significant enterprise risk and related to the Company’s core business. Indeed, each of Bock, Bingle, Boro, Hao, Hoffman, Kinney, Lines, Sundaram, and Widmann acknowledged the gravity of this risk in the Company’s Forms 10-K.

86. However, the Nominating and Corporate Governance Committee met only once during 2018 and only three times during 2019. Four meetings over the course of two years, by the only Board committee designated to oversee SolarWinds’ most significant enterprise risk supports and inference that the Company did not conduct adequate oversight of cyber and data security risks.

87. Worse, the Nominating and Corporate Governance Committee charter, most recently amended in February 2020, clearly does not vest the committee with the authority or responsibility to the Company’s policies, plans and programs relating to cyber and data security associated with SolarWinds’ products and business operations. The committee’s responsibilities as defined by the charter do not include oversight of any enterprise risks:

The primary responsibilities of the Committee are to (i) identify individuals qualified to become Board members; (ii) select, or recommend to the Board, director nominees for each election of directors; (iii) develop and recommend to the Board criteria for selecting qualified director candidates; (iv) consider committee member qualifications, appointment and removal; (v) recommend

corporate governance principles and a code of conduct applicable to the Company; and (vi) provide oversight in the evaluation of the Board and each committee.

88. The charter specifically identifies the committee's authority and responsibility as relating to only two subjects: nominating functions and "corporate governance functions." The corporate governance functions consist of eleven items, none of which relate to the Company's policies, plans and programs relating to cyber and data security associated with SolarWinds' products and business operations:

1. Develop, recommend for Board approval, and review on an ongoing basis the adequacy of, the Corporate Governance Guidelines applicable to the Company. Such principles shall include director qualification standards, director responsibilities, committee responsibilities, director access to management and independent advisors, director compensation, director orientation and continuing education, management succession and annual performance evaluation of the Board and committees.
2. Consult with the Financial Audit Committee regarding the Company's adoption of a Code of Business Conduct and Ethics applicable to all employees and directors, which meets the requirements of Item 406 of the SEC's Regulation S-K and the rules of the NYSE, and provide for and review prompt disclosure to the public of any change in, or waiver of, such Code of Business Conduct and Ethics. Review such Code of Business Conduct and Ethics periodically and recommend such changes to such Code of Business Conduct and Ethics as the Committee shall deem appropriate, and adopt procedures for monitoring and enforcing compliance with such Code of Business Conduct and Ethics.
3. Review, at least annually, the Company's compliance with the NYSE corporate governance listing requirements, and report to the Board regarding the same.
4. Assist the Board in developing criteria for the evaluation of Board and committee performance.
5. Oversee the evaluation of the performance of the Board, each committee of the Board and Company management.
6. Review and recommend to the Board changes to the Company's bylaws as needed.
7. Develop corporate governance-related continuing education for Board members.
8. Establish stock ownership guidelines for the Company's executive officers and non-employee directors if the Committee deems such guidelines appropriate, review compliance of executive officers and non-employee directors with

established guidelines, and periodically assess and revise such guidelines, as appropriate.

9. Make reports to the Board regarding the foregoing as appropriate.

10. Review and reassess the adequacy of this Charter as appropriate and recommend any proposed changes to the Board for approval.

11. Perform any other activities consistent with this Charter, the Company's Bylaws and governing law, as the Committee or the Board deems necessary or appropriate.

89. Thus, the Board utterly failed to implement any system for Board oversight of the Company's policies, plans and programs relating to cyber and data security. While the Board claims in its proxy statements that the Nominating and Corporate Governance Committee oversees the Company's policies, plans and programs relating to cyber and data security on behalf of the Board, the Nominating and Corporate Governance Committee does not even have the authority to oversee such policies, plans and programs and is not responsible for doing so. Were the Nominating and Corporate Governance Committee actually engaged in oversight of cyber and data security, it would have met more than four times during all of 2018 and 2019.

90. The Board's professed system for oversight of cyber and data security was a committee that met only sporadically, devoted patently inadequate time to its work, and did not even have the authority to conduct the oversight over the very risks the Board claimed it was overseeing. Bock, Bingle, Boro, Hao, Hoffman, Kinney, Lines, Sundaram, and Widmann therefore breached their fiduciary duties by a sustained or systemic failure to exercise oversight over cyber and data security. because they failed to ensure the Board had any functioning system of overseeing these major enterprise risks.

**B. Additional Reasons Demand is Excused**

91. Bock, Howard, Kinney, and Sundaram served as the members of the Audit Committee at relevant times. As such, they are responsible for the effectiveness of the Company's

internal controls, the integrity of its financial statements, and its compliance with laws and regulations. In their capacities as Audit Committee members, Bock, Howard, Kinney, and Sundaram reviewed and approved the disclosures regarding the Company's cybersecurity risks. As alleged herein, Bock, Howard, Kinney, and Sundaram failed to ensure the integrity of the Company's internal controls, allowing the materially misleading statements to be disseminated in SolarWinds's SEC filings and other disclosures. Thus, Bock, Howard, Kinney, and Sundaram breached their fiduciary duties and are not disinterested, and demand is excused as to them.

92. Bingle, Boro, Hao, and Lines served on the Board when the Company's cybersecurity advisor provided a presentation in 2017 stating that SolarWinds' system required improvements to protect against future attack. These directors knowingly or recklessly ignored the clear indicators of vulnerabilities in the cybersecurity system, and their failure to take action is a breach of fiduciary duty, and demand is excused as to them.

### **COUNT I**

#### **Against Defendants Thompson and Kalsu for Breach of Fiduciary Duty**

93. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

94. Defendants Thompson and Kalsu each owes and owed to the Company the duty to exercise candor, good faith, and loyalty in the management and administration of SolarWinds's business and affairs, particularly with respect to issues as fundamental as public disclosures.

95. The conduct by defendants Thompson and Kalsu set forth herein was due to their intentional or reckless breach of the fiduciary duties they owed to the Company. Defendants Thompson and Kalsu intentionally or recklessly breached or disregarded their fiduciary duties to protect the rights and interests of SolarWinds.

96. In breach of their fiduciary duties owed to SolarWinds, defendants Thompson and Kalsu willfully participated in and caused the Company to expend unnecessarily its corporate funds, rendering them personally liable to the Company for breaching their fiduciary duties.

97. In particular, defendants Thompson and Kalsu knowingly or recklessly made untrue statements and/or permitted the Company's public filings, disclosures, and statements to misleadingly report revenue and the Company's overall prospects.

98. As a direct and proximate result of the breaches of their fiduciary obligations by defendants Thompson and Kalsu, SolarWinds has sustained and continues to sustain significant damages, including direct monetary damages, exposure to liability from securities litigation and a loss of goodwill in the capital markets. As a result of the misconduct alleged herein, defendants are liable to the Company.

## **COUNT II**

### **(Against Defendants Thompson, Bock, Bingle, Boro, Hao, Hoffman, Kinney, Lines, Sundaram, Widmann, and Cormier for Violations of Section 14(a) of the Exchange Act)**

99. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

100. Rule 14a-9, promulgated pursuant to § 14(a) of the Securities Exchange Act of 1934, provides that no proxy statement shall contain "any statement which, at the time and in light of the circumstances under which it is made, is false or misleading with respect to any material fact, or which omits to state any material fact necessary in order to make the statements therein not false or misleading." 17 C.F.R. § 240.14a-9. The Company's proxy statements filed on April 5, 2019 and April 9, 2020 violated § 14(a) and Rule 14a-9 because they materially misrepresented the Board's oversight of risk because the nominating and corporate governance committee was

only empowered to act as to nominating functions and eleven “corporate governance functions,” none of which included the oversight of any enterprise risks.

101. The misrepresentations and omissions in the proxy statements were material to Company shareholders evaluating the proxy statements. The 2019 proxy statement solicited and obtained shareholder votes for director nominees and the ratification of the appointment of the Company’s independent auditor. The 2020 proxy statement solicited and obtained shareholder votes for: (i) director nominees; (ii) ratification of the appointment of the Company’s independent auditor; and (iii) the frequency of advisory votes on executive compensation. The proxy statement was an essential link in the Individual Defendants’ continued breaches of fiduciary duty.

102. The misleading statements in the 2019 and 2020 proxy statements caused direct harm to SolarWinds and to its shareholders. Had the truth been revealed in the proxy statements, SolarWinds’ minority shareholders would have known that all of the misleading statements detailed herein were untrue, and they would have pursued state law remedies to halt the 2019 and 2020 annual meetings, such as suing for an injunction. Because the proxy statements misled them as to the Board’s risk oversight activities, they forewent their state law remedies and did not take action to halt the meetings, and the Sponsors’ continued ability to control the Board and confer equity compensation on the directors at the expense of the Company went unchallenged.

103. The Company was damaged as a result of the defendants’ material misrepresentations and omissions in the proxy statements.

### **COUNT III**

#### **(Against Defendants Thompson and Kalsu for Contribution For Violations of Sections 10(b) and 21D of the Exchange Act)**

104. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

105. The conduct of Defendants Thompson and Kalsu, as described herein, has exposed the Company to significant liability under various federal and state securities laws by their disloyal acts.

106. SolarWinds is named as a defendant in related securities fraud lawsuit that allege and assert claims arising under § 10(b) of the Exchange Act. The Company is alleged to be liable to private persons, entities and/or classes by virtue of many of the same facts alleged herein. If SolarWinds is found liable for violating the federal securities laws, the Company's liability will arise in whole or in part from the intentional, knowing, or reckless acts or omissions of all or some of the Defendants as alleged herein, who have caused the Company to suffer substantial harm through their disloyal acts. The Company is entitled to contribution and indemnification from these Defendants in connection with all claims that have been, are, or may be asserted against the Company by virtue of their wrongdoing.

107. As officers, directors and otherwise, Defendants Thompson and Kalsu had the power or ability to, and did, control or influence, either directly or indirectly, SolarWinds's general affairs, including the content of its public statements, and had the power or ability to directly or indirectly control or influence the specific corporate statements and conduct that violated § 10(b) of the Exchange Act and SEC Rule 10b-5.

108. Defendants Thompson and Kalsu are liable under § 21D of the Exchange Act, which governs the application of any private right of action for contribution asserted pursuant to the Exchange Act.

109. Defendants Thompson and Kalsu have damaged the Company and are liable to the Company for contribution.

110. No adequate remedy at law exists for Plaintiff by and on behalf of the Company.

**COUNT IV**

**Against Thompson, Kalsu, Bingle, and Lines – *Brophy* Claim**

111. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

112. As alleged above, Thompson, Kalsu, Bingle, and Lines are fiduciaries of SolarWinds, possessed material, non-public information of SolarWinds, and used that information improperly to profit from sales of SolarWinds stock. When Thompson, Kalsu, Bingle, and Lines directed the stock sales set forth above, they were motivated to do so, in whole or in part, by the substance of the material, non-public information they possessed, and they acted with scienter.

113. When Thompson, Kalsu, Bingle, and Lines sold their SolarWinds stock, they knew that the investing public was unaware of the negative material information that they possessed. They also knew that if the information were disclosed, the market price of SolarWinds stock would be significantly lower. Thompson, Kalsu, Bingle, and Lines timed their stock sales to take advantage of the investing public's ignorance of the concealed material facts and obtain a higher price for the stock they sold. They thereby benefitted by misappropriating SolarWinds's non-public information.

114. Plaintiff has no adequate remedy at law.

**COUNT V**

**Against the Defendants Bock, Bingle, Boro, Hao, Hoffman, Kinney, Lines, Sundaram, Widmann, and Cormier for Breach of Fiduciary Duty**

115. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.



116. These Defendants each owes and owed to the Company the duty to exercise candor, good faith, and loyalty in the management and administration of SolarWinds's business and affairs, particularly with respect to issues as fundamental as public disclosures.

117. These Defendants' conduct set forth herein was due to their intentional or reckless breach of the fiduciary duties they owed to the Company. These Defendants intentionally or recklessly breached or disregarded their fiduciary duties to protect the rights and interests of SolarWinds.

118. In breach of their fiduciary duties owed to SolarWinds, these Defendants committed a sustained failure to exercise oversight over SolarWinds' cyber and data security risks and failed to even implement a system for oversight of such risks. They thus acted in bad faith and caused the Company to expend unnecessarily its corporate funds, rendering them personally liable to the Company for breaching their fiduciary duties.

119. Addition, these Defendants knowingly or recklessly made untrue statements and/or permitted the Company's public filings, disclosures, and statements to misleadingly report revenue and the Company's overall prospects.

120. As a direct and proximate result of these Defendants' breaches of their fiduciary obligations, SolarWinds has sustained and continues to sustain significant damages, including direct monetary damages, exposure to liability from securities litigation and a loss of goodwill in the capital markets. As a result of the misconduct alleged herein, defendants are liable to the Company.

#### **PRAYER FOR RELIEF**

WHEREFORE, plaintiff, on behalf of SolarWinds, demands judgment as follows:

A. Declaring that plaintiff may maintain this action on behalf of SolarWinds and that plaintiff is an adequate representative of the Company;

B. Against all of the defendants and in favor of the Company for the amount of damages sustained by the Company as a result of the defendants' breaches of fiduciary duties, waste of corporate assets, and unjust enrichment;

C. Directing SolarWinds to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect SolarWinds and its stockholders from a repeat of the damaging events described herein, including, but not limited to, putting forward for stockholder vote, resolutions for amendments to the Company's Bylaws or Articles of Incorporation and taking such other action as may be necessary to place before stockholders for a vote of the following corporate governance policies:

1. a proposal to strengthen the Company's controls over financial reporting;
2. a proposal to strengthen the Board's supervision of operations and develop and implement procedures for greater stockholder input into the policies and guidelines of the Board;
3. a proposal to strengthen SolarWinds's oversight of its disclosure procedures;
4. a provision to control insider transactions; and
5. a provision to permit the stockholders of SolarWinds to nominate at least three candidates for election to the Board;

D. Extraordinary equitable and/or injunctive relief as permitted by law, equity, and state statutory provisions sued hereunder, including attaching, impounding, imposing a constructive trust on, or otherwise restricting the proceeds of defendants' trading activities or their other assets so as to assure that plaintiff on behalf of SolarWinds has an effective remedy;

E. Awarding to SolarWinds restitution from defendants, and each of them, and ordering disgorgement of all profits, benefits, and other compensation obtained by the defendants;

F. Awarding to plaintiff the costs and disbursements of the action, including reasonable attorneys' fees, accountants' and experts' fees, costs, and expenses; and

G. Granting such other and further relief as the Court deems just and proper.

**JURY DEMAND**

Pursuant to Fed. R. Civ. P. 38(b), plaintiff demands a trial by jury.

[Signatures on next page.]

Dated: March 25, 2021

By: /s/ Sammy Ford IV

Sammy Ford IV  
State Bar No. 24061331  
Jason S. McManis  
State Bar No. 24088032  
**AHMAD, ZAVITSANOS, ANAIPAKOS,  
ALAVI & MENSING P.C.**  
1221 McKinney St., Suite 2500  
Houston, TX 77010  
Telephone: (713) 600-4965  
Facsimile: (713) 655-0062  
E-Mail: sford@azalaw.com  
jmcmanis@azalaw.com

**GLANCY PRONGAY & MURRAY LLP**

Benjamin I. Sachs-Michaels  
712 Fifth Avenue  
New York, New York 10019  
Telephone: (212) 935-7400  
E-mail: mhouston@glancylaw.com  
bsachsmichaels@glancylaw.com

-and-

Robert V. Prongay  
Pavithra Rajesh  
1925 Century Park East, Suite 2100  
Los Angeles, California 90067  
Telephone: (310) 201-9150  
E-mail: rprongay@glancylaw.com  
prajesh@glancylaw.com


*Counsel for Plaintiff David Sobel*

**SOLARWINDS CORPORATION VERIFICATION**

I, David Sobel, do hereby verify that I am a holder of common stock of SolarWinds Corporation and was a holder of such common stock at the time of the wrongs complained of in the foregoing Verified Shareholder Derivative Complaint (the "Complaint"). I have reviewed and authorized the filing of the Complaint. All of the averments contained in the Complaint regarding me are true and correct upon my personal knowledge, and with respect to the remainder of the averments, are true and correct to the best of my knowledge, information and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Date: 3/17/2021

DocuSigned by:  
  
915CADEF21B94AA...  
David Sobel